DISCUSSION PAPER

Topic: Analyzing Risks for Continuity Planning – Linking Threats to Disruption Scenarios

1.0 Objectives of Risk Analysis

The activities of every organization and its assets, its staff, executives, facilities, equipment, databases, cash, and vendors are subject to disruptions from a wide range or variety of causes. In the big picture, every senior executive should consider potential causes of disruptions and their likely effects and consequences to identify means for preventing disruptions, mitigating their effects if they do occur, and minimizing their costs via collective sharing of risks (i.e., insurance). An additional motivation for analyzing risks is to design effective continuity plans.

Identifying, interpreting, and evaluating risks to an organization's operations is a key task in the planning and design of a continuity of operations and continuity of government (COOP/COG) plan. The manner in which this task is performed can influence significantly the shape and form that a continuity plan takes. In fact, a poorly executed risk analysis can lead to the development of a continuity plan that is totally ineffectual for the risks at hand, enormously expensive to develop and maintain, or both. This discussion addresses some of the difficulties and challenges that risk analysis pose to continuity of operations planning.

2.0 Basic Terms and Concepts

To minimize confusion in this discussion, the following terms are used to describe particular concepts:

- An organization's operations are disrupted when resources that they require such as people, communication systems, facilities, databases, computers with associated operating systems, utilities, software applications, and network or communications capabilities, specialized equipment, materials and supplies, or vendors – are not available when, where, and how they are normally expected.
- The unavailability of resources as they are normally expected is the effect of a cause, such as a power outage, a flood, a human "goof", a technology failure, a malicious act by an employee or contractor, or an act of terrorism.
- Causes of disruptions occur with some degree of randomness and unpredictability – they cannot be anticipated exactly in terms of time, place, and manner of occurrence.
- Disruptions of operations have consequences or effects: some of them may be minor or small, and others may be extremely large in their breadth of impact.
- A risk is the possibility that an operation will be disrupted by a cause that can create serious negative consequences;
- Prevention is a program of activity or actions that seek to reduce to zero the probability of a cause occurring.
- Mitigation is a program of activity or actions that seek to minimize the consequences of a cause when an occurrence is first detected.

- For some situations that occur with some degree of frequency and familiarity, a form of mitigation is a standard operating procedure (SOP) to address the cause and restore operating order quickly. SOPs are activated routinely and do not call for exceptional management decision-making.
- Situations whose consequences are so large that routine management policies and procedures are overwhelmed, and for which there are no contingency or continuity plans, require *ad hoc* decisions by senior executives who pre-empt routine management protocols. This situation requires crisis management.

Situations whose consequences are potentially so large that routine management policies and procedures will be overwhelmed, yet whose likelihood of occurring is "reasonable" and prevention and mitigation actions are not sufficient, are candidates for continuity planning. Continuity planning anticipates these causes and their consequences or effects on operations, and provides exceptional courses of action that organization executives and staff must undertake to address the situation. By documenting these needs in a plan, informing all key staff about the plan and even practicing or exercising the plan, the organization is prepared to respond, should a major disruption occur.

3.0 Identifying Causes and Effects

A key question that all continuity planners must address is how to describe the causes and effects of disruptions, and how to assess what is typically referred to as a risk analysis. The list of possible causes, with some reasonable minimum probability of occurrence, may be manageable in the sense that it is not enormous in length, and at least some rough estimates of probabilities of occurrence can be produced for each cause.

Difficulties arise when planners contemplate all of the possible combinations or permutations of effects that one or more causes can produce. Not only is this list potentially infinite (and well beyond the scope of most planning resources), but the work involved in estimating the impacts or consequences of each effect on operations is enormous. For each variation on how, say, a power outage occurs, or a flood occurs, or a malicious employee attacks the establishment, the planner must estimate the damages, considering all of the prevention, mitigation, and SOPs that might reduce the harm.

A separate discussion paper addresses in more detail the procedures for estimating the consequences or impacts that a disruption can have on an organization's activities. This area of study is called business impact assessment or analysis (BIA). For this discussion, it is sufficient to note that estimating the consequences of disruptions is not straight forward.

Nevertheless, governing bodies, entities, and authorities providing critical roles and services must both anticipate occasions of delivery degradation and plan to prevent, respond, mitigate, and recover from such instances. Sources for such disruptions include:

- Aircraft/Transportation Accidents
- Avalanches

- Civil Disorder
- Fire
- Drought
- Earthquakes
- Floods
- Hazardous Material Incidents
- Landslides
- Snowstorms
- Terrorism
- Tornados
- Tsunamis
- Volcanoes
- Wildfires
- Windstorms

These hazards may occur independently (e.g., tornado), concurrently (volcano, earthquake, and wildfire), or successively (e.g., snowstorms and avalanches), and are accompanied by a range of effects including:

- Area Denial/Contamination
- Death or injury of personnel (civilians or workers)
- Destruction of Property/Structural Damage
- Explosive Blast Wave / Shock Wave
- Fire
- Heat
- Loss of food/water
- Loss of transportation/communications/power
- Medical care lack of and / or surge capacity

The consequences of these effects can include:

- Economy – demise of business activity
- Evacuation – sustained loss of population
- Government – leadership and confidence lost
- Government Operations deteriorated

- Medical Services degraded
- Psychological and Sociological Impacts – traumatized public
- Safety – deterioration in law and order.

4.0 Grappling with Probabilities

The previous section considered the merits of explicitly considering all of the combinations of possibilities of how disruptions could occur, starting with an extensive but not overwhelming list of possible causes. Yet the combinations of effects and the wide range of possible consequences make the task daunting. Can the list be reduced by using more discrimination on acceptable probabilities? That is, maybe only the (relatively) few causes with reasonably high probabilities should be contemplated.

This approach has some merit, but it also contains a drawback, a "Catch-22". Restricting consideration of causes to the most likely ones may exclude some causes that are less likely to occur yet whose consequences could be severe. Yet one cannot assess the severity without performing the more extensive analysis. Further, some of the more likely causes may not create severe consequences, because prevention or mitigation actions are already in place.

While many executives may be tempted to conclude "it can't or won't happen to us," one only need consider some of the major disasters that have occurred in the last few years, recognizing that they can occur in many locations occupied by American organizations:

- Terrorist attacks of 9/11/2001, thousands of lives lost (and terrorist attacks worldwide have increased in number each year since);
- Tsunami hits Indian Ocean, massive destruction of property and over 100,000 lives lost.
- Hurricane Katrina hits Gulf Coast in 2005, massive destruction of broad area, including a major metropolitan area, and deaths numbering over one thousand;

Although the likelihood of terrorist acts occurring appears to be smaller than other natural or "man-made" events (such as region-wide power outages), the nature of the terrorist threat is growing.

5.0 Software Solutions – and Compromises

Having considered some of the challenges in analyzing risks to operations, it must be said that some risk analysts have developed software that facilitates the analysis of risks posed by many different causes and estimates the consequences to operations. Some of these tools go so far as to provide probability distributions and offer output measures, such as expected levels of damage and worst case or maximum damage estimates. As the previous points of

discussion illustrate, however, one must ask what compromises or assumptions are built into the software regarding such issues as:

- The extensiveness of the list of possible causes of disruptions;
- The observational basis for assigning probabilities of occurrence to the disruptions;
- How the probability values are altered if/when the user identifies a source of risk that: a) has been present all along but, b) was not included specifically in the original list;
- How the software estimates the effect of a cause on a business process;
- How the software estimates the consequences of effects for a given business process.

The difficulty in answering the questions above is that the user must calibrate the automated analysis to be confident that it is providing realistic assessments of the planner's own situation. The most effective approach is to establish that the analytical "model" has been applied repeatedly and successfully to circumstances highly comparable to the planner's own organization and operating environment.

6.0 A Simple Approach

Some planners adopt a very simple approach to risk analysis that is quite acceptable to some senior executives for some circumstances. This approach starts with a set of basic disruption scenarios that summarize or encapsulate the effects of a wide range of possible causes:

- Loss of access to facilities, via highly localized causes (so that nearby facilities are not affected and may serve as alternatives);
- Loss of access to facilities, via causes affecting wide areas (and precluding recovery via nearby facilities);
- Loss of communications systems (typically, one or two systems that may be co-dependent, but not all systems at once, assuming that most systems are provided and operated independently);
- Loss of computing systems (databases, software applications, servers and operating system platforms, and/or networks);
- Loss of key and critical staff;
- Loss of highly specialized equipment;
- Loss of key and critical vendors or other services provided inter- or intra-organization.

This initial list of disruption scenarios may then be compared with a list of possible and probable causes of disruptions. The purpose of this comparison or review is two fold:

1. To identify all causes that are of singular importance to the organization's operating environment yet not addressed adequately by these scenarios, individually or collectively. If such causes surface, then new scenarios may be introduced.
2. To eliminate scenarios that are extremely unlikely to occur, because no causes with corresponding effects can be identified (e.g., some computing systems may already contain sufficient redundancy or resiliency, the result of previous risk assessments).

Having finalized a list of "reasonable" scenarios, each essential function or operation of the organization is examined in the context of these scenarios to estimate the total impact or consequences from each scenario. Those scenarios that threaten much harm become the preliminary basis for designing continuity recovery plans and strategies.

The thrust of this approach emphasizes continuity planning as an organizational process for responding to many possible causes of disruptions. Experience reveals that rarely does any disruption occur exactly as envisioned in any given scenario, and the role of a continuity plan is to prepare the executives and staff to analyze and respond quickly to each disruptive event as it unfolds.

In some cases, the initial estimates for developing or implementing a continuity plan's capabilities can be overwhelming or simply beyond reason. In these circumstances, planners may return to the task of comparing causes and scenarios, and perhaps introduce rough estimates of probabilities of causes, in an effort to reduce the requirements of a plan. At this stage, too, they may re-examine their estimates of potential impacts via a BIA.

7.0 SUMMARY

A challenge encountered by continuity planners is becoming too wrapped up in the complexities of risk analysis. Causes of disruptions to operations, the probabilities of causes occurring, the effects of causes if they do occur, and the consequences of the effects all become entangled and can blur the objectives of a continuity plan. Yet without some basis for guiding the development of a continuity plan, its expected effectiveness can't be estimated, nor can planners know how to design tests for exercising it.

A simple approach outlined here starts with adoption of a very limited set of basic disruption scenarios. These scenarios are compared with a list of possible disruption causes that are realistic for the planner's environment. The most important scenarios are then considered for all essential functions, to estimate the total harm that each scenario could cause. The continuity plan then addresses the most harmful scenarios by formulation of effective recovery strategies.